IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Robin Pou et al.	Art Unit	: 3685
Serial No.	: 10/726,284	Examiner	: John M. Winter
Filed	: December 2, 2003	Conf. No.	: 5291
Title	: DISTRIBUTION AND RIGHTS MANAGEMENT OF DIGITAL CONTENT		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

Appellants file this brief on appeal under 37 CFR 41.37, thereby perfecting the Notice of Appeal originally filed on February 9, 2009 after the Final Office Action dated October 8, 2008 ("Final Action") and the Advisory Action dated February 3, 2009 ("Advisory Action").

(1) Real Party in Interest

PAN Asset Acquisition, LLC, is the real party in interest.

(2) Related Appeals and Interferences

There are no related appeals or interferences.

(3) Status of Claims

Claims 1-19 and 74-84 have been cancelled, claims 20-48, 55-59, 63-73, 85-99, 104-107 and 113-118 are withdrawn, and claims 49-54, 60-62, 100-103 and 108-112 are pending, with 49, 60, 100, and 108 being independent. All pending claims stand rejected, and all appending claims are on appeal.

(4) Status of Amendments

All amendments have been entered and no amendments are being submitted herewith.

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: October 14, 2009.

(5) Summary of Claimed Subject Matter

Independent claim 49 is directed to a method for managing digital rights, wherein an input/output system of a user device is monitored for attempted file transfers. *See*, *e.g.*, Present *Application* at 5:15-24; 9;23-25; 10:27-11:3; 30:12-31:2; FIG. 1 and 8. The method then detects an attempt to transfer a data file between the user device and an external device through one of the input/output ports of the user device, wherein the data file is stored in an unwrapped form prior to the attempt to transfer the data file. *See*, *e.g.*, *id.* at 5:15-24; 9;23-25; 10:27-11:3; 30:12-31:2; FIG. 1 and 8; *see also id.* at 22:4-14; FIG. 4. Next, the method applies a digital wrapper to the unwrapped data file in response tot the detected attempt to transfer the data file before allowing the attempted transfer, wherein the digital wrapper is adapted to prevent unauthorized access to the data file after the data file is transferred between the user device and the external device. *See*, *e.g.*, *id.*; *see also* at 22:15-23:18; FIG. 4.

Independent claim 60 is also directed to a method for managing digital rights. This method identifies a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution. *See*, *e.g.*, *id.* at 5:15-24; 10:27-11:3; 22:4-14; 30:12-31:2; FIG. 1, 4 and 8. Next, the method identifies access rules associated with the media file, where the access rules include information relating to usage rights and usage fees. *See*, *e.g.*, *id.* at 5:20-24; 30:12-31:2; 31:12-30; 32:1-28; FIG. 8 and 9. Finally, the method applies a digital wrapper to the media file before distribution occurs, where the digital wrapper includes identification data for the media file and data related to the access rules, and further, where the digital wrapper is adapted to prevent unauthorized access to the media file after the media file is distributed to the external device. *See*, *e.g.*, *id.* at 5:15-24; 9;23-25; 10:27-11:3; 22:4-14; 30:12-31:2; FIG. 1, 4, and 8.

Independent claim 100 is directed to an article comprising a machine-readable medium storing instructions for causing one or more processors to perform a number of operations. *See*, *e.g.*, *id.* at 34:1-35:11. The first operation of the article comprises monitoring an input/output system of a user device for attempted file transfers between the user device and an external device through one or more input/output ports of the user device. *See*, *e.g.*, *id.* at 5:15-24; 9;23-25; 10:27-11:3; 30:12-31:2; FIG. 1 and 8. Next, the article detects an attempt to transfer a data file between the user device and an external device through one of the input/output ports of the

user device, wherein the data file is stored in an unwrapped form prior to the attempt to transfer the data file. *See*, *e.g.*, *id.* at 5:15-24; 9;23-25; 10:27-11:3; 30:12-31:2; FIG. 1 and 8; *see also id.* at 22:4-14; FIG. 4. Then, the article applies a digital wrapper to the unwrapped data file in response to the detected attempt to transfer the data file before allowing the attempted transfer, wherein the digital wrapper is adapted to prevent unauthorized access to the data file after the data file is transferred between the user device and the external device. *See*, *e.g.*, *id.*; *see also* at 22:15-23:18; FIG. 4.

Independent claim 108 is directed to an article comprising a machine-readable medium storing instructions for causing one or more processors to perform a number of operations. *See*, *e.g.*, *id.* at 34:1-35:11. The first operation is identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution. *See*, *e.g.*, *id.* at 5:15-24; 10:27-11:3; 22:4-14; 30:12-31:2; FIG. 1, 4 and 8. Next, the article performs an operation for identifying access rules associated with the media file, where the access rules include information relating to usage rights and usage fees. *See*, *e.g.*, *id.* at 5:20-24; 30:12-31:2; 31:12-30; 32:1-28; FIG. 8 and 9. Finally, the article applies a digital wrapper to the media file before distribution occurs, where the digital wrapper includes identification data for the media file and data related to the access rules, and further, where the digital wrapper is adapted to prevent unauthorized access to the media file after the media file is distributed to the external device. *See*, *e.g.*, *id.* at 5:15-24; 9;23-25; 10:27-11:3; 22:4-14; 30:12-31:2; FIG. 1, 4, and 8.

(6) Grounds of Rejection to be Reviewed on Appeal

Whether claims 49-54, 60-62, 100-103, and 108-112 are unpatentable over U.S. Patent No. 6,044,469 ("*Boebert*") in view of U.S. Patent No. 6,226,618 ("*Downs*") and further in view of U.S. Patent No. 4,740,890 ("*William*") under 35 U.S.C. §103(a).

(7) Argument

Claims 49-54, 60-62, 100-103, and 108-112 stand rejected under 35 U.S.C §103(a) as being unpatentable over U.S. Patent No. 6,044,469 ("*Boebert*") in view of U.S. Patent No. 6,226,618 ("*Downs*") and further in view of U.S. Patent No. 4,740,890 ("*William*").[1] Appellants respectfully disagree that the claims are obvious and assert that these rejections are improper.

I. Previous Office Actions Have Not Addressed the Specific Elements of the Currently Pending Independent Claims

Appellants submit that neither the Final Action nor the Advisory Action have addressed the arguments and claim amendments with regards to independent claims 49, 60, 100, and 108 set forth in both Appellants' Amendment in Reply to Action of April 4, 2008 and Reply to Final Action of October 8, 2008. Specifically, the Advisory Action and Final Action have failed to differentiate between the elements of independent claims 49 and 60[2] and now-cancelled independent claim 1, stating instead that "Claims 49 [and] 60…are not patentably distinct from claim 1 and are rejected for at least the same reasons[.]" Office Action, p. 4. In previous responses, Appellants have explicitly noted that Claims 49 and 60 recite different claim elements than those recited in now-cancelled independent claim 1, and that the subsequent office actions have failed to offer any reasoning or support for the continued rejections of the other independent claims.[3]

Claim 1, at the time of its cancellation, recited the following:

> 1. A method for managing digital rights, the method comprising:
> detecting a data file on a user device, wherein the data file includes a digital wrapper preventing access to the data file without a valid authorization;

---

[1] Appellants note that claims 1-19 and 74-84 have been cancelled, while claims 20-48, 55-59, 63-73, 85-99, 104-107 and 113-118 have been previously withdrawn. These remarks only address pending claims 49-54, 60-62, 100-103 and 108-112.

[2] Independent claim 100 contains certain aspects analogous to claim 49, while independent claim 108 recites certain aspects analogous to claim 60.

[3] Specifically, Appellants cancelled independent claim 1 in the Response to Final Action mailed December 22, 2008, leaving only independent claims 49, 60, 100, and 108 pending in the Present Application. Although the elements of the remaining independent claims differ from those of cancelled claim 1, no arguments or rejections addressing the remaining independent claims has been provided. For example, the Advisory Action's rejection of the pending claims merely states that "the Applicants argument fails to overcome the prior art rejection" without any explanation or rebuttal in response to Appellants' multiple arguments submitted in the Response to Final Action.

determining whether the user device includes software for disabling the digital wrapper, with the determination being made using executable instructions associated with the digital wrapper;

searching for information relating to an authorization to access the data file using data stored in a non-volatile storage area of the user device;

identifying information relating to an authorization to access the data file; and

disabling the digital wrapper based on the authorization.

Claim 49 and Claim 60, however, recite elements that were never included in claim 1 and which have not been specifically rejected by any of the previous rejections, nor had any portions of the cited references identified as specifically teaching or suggesting the respective claim elements. For example, Claim 49 recites "detecting an attempt to transfer a data file between [a] user device and an external device," that the "data file is stored in an unwrapped form prior to the attempt to transfer the data file," and "applying a digital wrapper to the unwrapped data file in response to the detected attempt to transfer the data file." Similarly, Claim 60 recites "identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution" and "applying a digital wrapper to the media file before distribution occurs." Each of these example elements are absent from now-cancelled independent claim 1.

Appellants submit that each and every element of the pending independent claims has not been adequately addressed in previous office actions.

II. Independent Claims 49, 60, 100 and 108 are Allowable Over the *Boebert-Down-William* Combination

While the previous actions have failed to provide any arguments or rejections addressing the specific elements of independent claims 49 and 100 unique from cancelled claim 1, Appellants submit that – regardless of the failure to provide justification for the previous rejections – *Boebert*, *Downs*, and *William*, either alone or in combination, fail to teach or suggest each and every element of the independent claims.

Generally, claim 49 is directed to the problem of preventing data files from being copied off of a user device to some external device where the data file is subject to unauthorized access, while still allowing the data file to remain freely accessible within a user device on which it

resides for authorized use. Accordingly, when a transfer of a data file is attempted, the file is wrapped to prevent unauthorized access after the file is actually transferred. Thus, after the transfer, access to the file can be limited to authorized users and/or authorized devices by the applied digital wrapper. Neither *Boebert*, *Downs*, nor *William* teach or suggest storing a data file in an unwrapped form on a user device prior to an attempt to transfer the data file and applying a digital wrapper to the unwrapped data file in response to detecting an attempt to transfer the data file before allowing the attempted transfer as recited in claim 49.

Boebert, for example, is directed to a data communication system including a secure processing unit that communicates with a personal keying device and a crypto media controller attached to a user's computer. *See Boebert*, Abstract. Communication between elements of the system creates keys, identifiers, and attributes used to identify and authenticate the user, assign user security access rights and privileges, and assign media and device attributes to a data access device according to a predefined security policy. *Id.* *Boebert*, however, seems to at least teach away from storing a data file in an unwrapped form on a user device prior to an attempt to transfer the data file, instead teaching that access to files within a unit of media is allowed only "at the last possible moment" using a "combination of an 'access vector' assigned to an individual and the 'device attributes' assigned to a particular Workstation." *Id.* at 3:20-24. In other words, *Boebert's* media is stored in encrypted form before, during, and after any transfer. Thus, *Boebert* fails to teach or suggest that files are stored in an unwrapped form on a user device, where a digital wrapper is applied to the file in response to detecting an attempt to transfer the data file.

Downs, on the other hand, discloses a system and related tools for the secure delivery and rights management of digital assets. *See Downs*, Abstract. However, *Downs* explicitly teaches away from the claim 49 elements of storing a data file in unwrapped form and in response to an attempt to transfer the data file, applying the digital wrapper, instead teaching the enforcement of content usage conditions as performed by the following steps:

> "First, upon reception of the Content 113 copy…the End-User Device(s) 109 marks the Content 113 with a Copy/Play Code 523 representing the initial copy/play permission. Second, the Player Application 195 cryptographically scrambles the Content 113 before storing it in the End-User Device(s) 109. The Player Application 195 generates a scrambling key for each Content Item, and the

> key is encrypted and hidden in the End-User Device(s) 109. Then, every time the End-User Device(s) 109 accesses the Content 113 for copy or play, the End-User Device(s) 109 verifies the copy/play code before allowing the de-scrambling of the Content 113 and the execution of the play or copy."

Downs, 21:43-63 (emphasis added). In direct contrast to claim 49, *Downs* describes that content is encrypted and stored (in an encrypted form) on the user device immediately upon receiving the content, requiring the content to be decrypted and verified before any access for copy or play on the user device.

Further, *William* discloses an apparatus for preparing and using software during a trial period associated with the software. *See William*, Abstract. *William* also teaches away from storing a data file in an unwrapped form on a user device prior to an attempt to transfer the data file and wrapping the file in response to a detected attempt to transfer the content, instead describing that whenever a new version of the trial software is created, that version is associated with a "usage count…, [a] lock condition as to whether [the software] is locked or unlocked…and the output code for the disk..." *Id.* at 3:39-43. As the trial software is run on a computer, the system determines whether the trial software is locked, and if it is not locked, whether the usage count, or predetermined number of available uses, is zero. *See id.* at 4:13-29. The usage count is decremented with each use of the trial software, until the usage count reaches zero, wherein the trial software is no longer executable without providing an unlock code associated with the particular version of the trial software received from a third party, such as the software manufacturer or distributor. *See id.* at 4:37-5:2. In other words, *William* teaches that the trial software is received by the associated user or system in a protected format (that defines and enforces the trial period), and not that trial software is "stored in an unwrapped form prior to the attempt to transfer the [content]" and wrapped "in response to a detected attempt to transfer the [content]" as recited by claim 49. For at least these reasons, the *Boebert-Downs-William* combination fails to teach or suggest each and every element of claim 49.

Accordingly, Appellants respectfully request reconsideration and allowance of claim 49. Further, claims 60, 100, and 108 include certain aspects analogous to claim 49 and are allowable for at least the reasons discussed above.

CONCLUSION

For at least the reasons described above, the *Boebert-Down-William* combination fails to teach or suggest each and every element of the independent claims. Accordingly, Appellants respectfully request reconsideration and allowance of the independent claims and all claims depending therefrom.

Should the Board be of the opinion that a claim on appeal may be amended to overcome a specific rejection, the Board is respectfully requested to include in the opinion such a statement and afford Appellants the right to amend in conformity therewith.

A Petition for a five-month extension of time accompanies this Appeal Brief. The small entity fee for a five-month extension of time in the amount of $1,175.00 and the Appeal brief fee in the amount of $270 are being paid concurrently herewith on the Electronic Filing System (EFS) by way of Deposit Account Authorization. Please apply any other charges or credits to Deposit Account No. 06-1050, referencing the above attorney docket number

Respectfully submitted,

Date: October 14, 2009

/Jonathan A. Solomon/
Jonathan A. Solomon
Reg. No. 64,869

Fish & Richardson P.C.
1717 Main Street, Suite 5000
Dallas, TX 75201
Telephone: (214) 747-5070
Facsimile: (877) 769-7945

Appendix of Claims

49. A method for managing digital rights, the method comprising:

monitoring an input/output system of a user device for attempted file transfers;

detecting an attempt to transfer a data file between the user device and an external device through one of the input/output ports of the user device, wherein the data file is stored in an unwrapped form prior to the attempt to transfer the data file; and

applying a digital wrapper to the unwrapped data file in response to the detected attempt to transfer the data file before allowing the attempted transfer, wherein the digital wrapper is adapted to prevent unauthorized access to the data file after the data file is transferred between the user device and the external device.

50. The method of claim 49 wherein the data file comprises a media file.

51. The method of claim 49 further comprising identifying the data file as embodying a particular protected work from a plurality of predetermined works, wherein the digital wrapper is applied based on the identity of the data file.

52. The method of claim 51 wherein the digital wrapper is applied based on the identity of the data file matching an identification of the data file in a database on the user device.

53. The method of claim 51 wherein identifying the data file comprises using a file recognition algorithm adapted for identifying data files as embodying particular protected works based on characteristics of the data files.

54. The method of claim 49 wherein the digital wrapper includes information identifying the data file and information relating to an allocation of credits to one or more distributors of the data file based on purchases of the data file.

60. A method for managing digital rights, the method comprising:

identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution;

identifying access rules associated with the media file, wherein the access rules include information relating to usage rights and usage fees;

applying a digital wrapper to the media file before distribution occurs, with the digital wrapper including identification data for the media file and data relating to the access rules, wherein the digital wrapper is adapted to prevent unauthorized access to the media file after the media file is distributed to the external device.

61. The method of claim 60 wherein the digital wrapper is adapted to be disabled for use of the media file by an external device that has a license to access the media file.

62. The method of claim 60 wherein the digital wrapper further includes information relating to at least one distributor of the media file.

100. An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

monitoring an input/output system of a user device for attempted file transfers between the user device and an external device through one or more input/output ports of the user device;

detecting an attempt to transfer a data file between the user device and an external device through one of the input/output ports of the user device, wherein the data file is stored in an unwrapped form prior to the attempt to transfer the data file; and

applying a digital wrapper to the unwrapped data file in response to the detected attempt to transfer the data file before allowing the attempted transfer, wherein the digital wrapper is adapted to prevent unauthorized access to the data file after the data file is transferred between the user device and the external device.

101. The article of claim 100 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising identifying the data file as being subject to protection from unauthorized copying.

102. The article of claim 101 wherein identifying the data file as being subject to protection from unauthorized copying includes locating an identifier for the data file in a database stored on the user device.

103. The article of claim 101 wherein identifying the data file as being subject to protection from unauthorized copying includes:

sending a message including information for identifying the data file to a remote server; and

receiving a response to the message indicating that the data file is subject to protection from unauthorized copying.

108. An article comprising a machine-readable medium storing instructions for causing one or more processors to perform operations comprising:

identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution;

identifying access rules associated with the media file, wherein the access rules include information relating to usage rights and usage fees;

applying a digital wrapper to the media file before distribution occurs, with the digital wrapper including identification data for the media file and data relating to the access rules, wherein the digital wrapper is adapted to prevent unauthorized access to the media file after the media file is distributed to the external device.

109. The article of claim 108 wherein identifying the media file comprises identifying the media file using a file recognition algorithm.

110. The article of claim 108 wherein identifying the access rules associated with the media file comprises receiving access rules from a remote server.

111. The article of claim 108 wherein the machine-readable medium stores instructions for causing one or more processors to perform further operations comprising:

receiving a request from a user of the external device for authorization to access the media file after distribution of the media file from the user device;

notifying a remote server of the request for authorization to access the media file by the external device; and

disabling the digital wrapper to allow access to the media file by the user of the external device.

112. The article of claim 108 wherein identifying the access rules associated with the media file comprises receiving the access rules from the user device.

Evidence Appendix

None.

Related Proceedings Appendix

None.